# ANONYMOUS ACQUISITION OF DIGITAL PRODUCTS BASED ON SECRET SPLITTING

## FIELD OF THE INVENTION

The present invention relates generally to electronic commerce systems and, in particular, to the anonymous acquisition of digital products within such electronic commerce systems.

## BACKGROUND OF THE INVENTION

Electronic commerce is increasingly becoming a part of everyday life. In particular, the rapid growth of the Internet and World Wide Web has lead to a corresponding increase in the ability to acquire goods and services remotely. A generalized example in accordance with current techniques is illustrated in FIG. 1. In particular, an entity 102, such as an individual or organization, may communicate with a provider 104 via a public network 103. The entity 102 transmits a variety of information to the provider 104 in order to acquire a product being offered by the provider 104. The information sent by the entity 102 typically comprises an identification of the entity, an identification of the product being acquired and, optionally, information regarding the price of the product being acquired. In turn, where the acquisition is a purchase, the provider 104 may supply some or all of the information from the entity 102 to a credit agency 106. As a result, the provider 104 has specific knowledge of the products being purchased by the entity 102. Likewise, the credit agency 106 has specific knowledge that the entity 102 is purchasing products from the provider 104. While this information may be valuable to the provider, an increasing number of consumers object to commercial entities and other third parties having specific knowledge of their purchasing habits.

The desire for privacy has lead to an increase in a number of services that maintain in secret the identity of users of those services. For example, a variety of anonymous e-mail services are currently available whereby recipients of an e-mail are not able to associate the sending entity's identification with the e-mail. While such services help maintain privacy, they also provide a means by which malicious parties may act more freely. Furthermore, in a purchase transaction, such anonymity could be used to perpetuate fraud against vendors. Therefore, a need exists for technique that provides enhanced privacy during e-commerce transactions, but that also provides a degree of accountability such that the opportunity for malicious acts is minimized.

## SUMMARY OF THE INVENTION

Anonymous acquisition of a digital product by an entity includes the method and apparatus that receives from the entity a plurality of acquisition-related variables necessary for the entity to acquire the digital product. At least some of the plurality of acquisition-related variables are split into a corresponding at least one set of variable secret shares. For each of the at least one set of variable secret shares, the set of variable secret shares is sent to a set of shareholders for long-term storage of the acquisition-related variables. Acquisition of the digital product by the entity is fulfilled based on the plurality of acquisition-related variables such that a provider of the digital product is unable to identify the entity.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a typical arrangement used in electronic commerce in accordance with prior art techniques.

FIG. 2 is a block diagram illustrating an arrangement that may be used for electronic commerce in accordance with the present invention.

FIG. 3 is a flow chart illustrating a technique in accordance with the present invention.

FIGS. 4-7 illustrate operation of an anonymity service in accordance with an embodiment of the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a technique for anonymously conducting electronic commerce transactions while simultaneously providing a means for auditing or memorializing such transactions if later required. In the context of the present invention, electronic commerce encompasses substantially all scenarios in which an acquirer of a digital product desires privacy, such as purchases, free downloads of software, etc. In particular, the present invention employs secret sharing techniques whereby information provided by an acquiring entity is kept confidential and yet accessible when required to fulfill the acquisition of a product via a public network such as the Internet or World Wide Web. An entity desiring to acquire a digital product from a provider supplies acquisition-related data such as an entity identification, information identifying the digital product and a provider of the product and, if applicable, a price of the product to an anonymity service. In turn, the anonymity service splits each of these pieces of information into a plurality of secret shares that are thereafter provided to corresponding sets of shareholders. The nature of the secret splitting process is such that each shareholder is unable to reproduce the secret corresponding to the shareholder's share without the other shareholders involved in the process. The anonymity service retains a transaction identification and identities of the shareholders, but does not store or otherwise retain the secrets, i.e., the acquisition-related data. When needed, the anonymity service reconstructs each piece of information by requesting the secret shares from the shareholders such that it can anonymously fulfill the acquisition of the product. In one embodiment of the present invention, the anonymity service verifies an acquiring entity's credit without identifying the particular product being acquired by the entity. Likewise, in another embodiment of the present invention, the anonymity service fulfills acquisition of the product from the product provider without identifying the entity acquiring the product. If later required, the anonymity service may reconstruct the secrets for the purposes of auditing, legal investigations or the like. By storing secret shares with a plurality of shareholders, the present invention facilitates anonymous transactions via public networks such as the Internet and World Wide Web while still accommodating the need for accountability.

The present invention may be more readily described with reference to FIGS. 2-7. Referring now to FIG. 2, there is illustrated a block diagram of a system 200 in accordance with the present invention. In particular, an anonymity service 203 is provided as an intermediary between the entity 202 and provider 204. Additionally, the anonymity service is in communication with a plurality of shareholders 207, a clearing house 205 and a credit agency 206. Although direct connections are illustrated between the anonymity service 203 and the various other elements of the system 200, it is understood that these connections may comprise paths established through public networks such as the Internet or World Wide Web, within private networks or through a combination of public and private networks.

In the context of the present invention, each of a plurality of entities 202 (one shown) may comprise any individual or organization capable of acquiring a digital product from the provider 204. In practice, each entity 202 communicates with the anonymity service 203 via a computer implementing a network communication program, such as a browser or the like. The provider 204, in turn, may likewise comprise any individual or organization that provides digital products via a communication network. In the context of the present invention, digital products comprise anything capable of delivery via a communication network. For example, digital products may include downloadable software or digital data such as text, audio, video or images. Those having ordinary skill in the art will recognize that other types of digital products may be used in conjunction with the present invention, and the present invention is not limited in this regard.

The anonymity service 203 preferably comprises a computer-implemented service available via a communication network such as the Internet or World Wide Web. As depicted in FIG. 2, the anonymity service 203 preferably comprises a processor 210 and memory 212. For example, the anonymity service may be implemented using one or more network servers executing stored software routines as known in the art. A more detailed description of operation of the anonymity service 203 is provided below with reference to FIGS. 3-7.

The anonymity service 203 is in communication with a plurality of shareholders 207 and a clearing house 205. As described in greater detailed below, each of the shareholders 207 is provided with a secret share which, by itself, does not

enable an individual shareholder to reconstruct a secret. Preferably, for each secret involved in a given transaction, there exists a separate set of shareholders used to maintain secret shares about that secret. The number of shareholders in each set of shareholders can be equal, although this is not a requirement. As a matter of design choice, each set of shareholders may be completely independent from all other sets of shareholders, or they may share any number of common members to the point where they are identical. In any event, each shareholder is capable of receiving secret shares from the anonymity service 203. To this end, each shareholder preferably comprises a computer-implemented device capable of communicating with the anonymity service 203. Because secret sharing schemes are vulnerable to the extent that separate shareholders could collaborate to ascertain the secret in their possession, it is advantageous to maintain the identity of each shareholder in confidence from the other shareholders. Furthermore, it is preferred to select the shareholders such that they have an inherent reason not to collaborate with each other. For example, shareholders in possession of the secret shares corresponding to a single secret may comprise competitors in a given industry. Such competitors are inherently unlikely or unwilling to share information with each other. Additionally, the shareholders may comprise a privacy organization that is dedicated to advocating privacy in electronic commerce, and therefore unlikely to collaborate with other shareholders. Further still, the entity 202 may comprise one of the shareholders, or the shareholders 207 may be known to the entity 202, such as family members or friends.

The clearing house 205 comprises a computer-implemented service used to credit an account of the provider 204 in those instances in which the transaction between the entity 202 and the provider 204 is a purchase of a digital product. The credit agency 206 comprises a computer-implemented credit verification service used when a digital product is being purchased by the entity 202. Together, the clearing house 205 and credit agency 206 allow the anonymity service 203 to anonymously fulfill a purchase request from the entity 202. This is described in greater detail below with reference to FIGS. 4-7.

Referring now to FIG. 3, a method in accordance with the present invention is illustrated. In particular, the method of FIG. 3 is preferably implemented by the anonymity service 203. Thus, at block 302 the anonymity service securely receives

acquisition-related variables necessary for an entity to acquire a digital product. Security in the transmission of the acquisition-related variables may be provided using known techniques, such as encryption or a trusted path. In the context of the present invention, the acquisition-related variables comprise an entity identification, identifications of a provider of a digital product as well as the digital product itself, and in those instances in which the acquisition is a purchase, a purchase price. The entity identification may comprise any unique identifier such as a public key, credit card number or the like. Likewise, the identifications of the provider and product may comprise any identifiers uniquely associated with the provider and product, respectively. Those having ordinary skill in the art will appreciate that a greater or lesser number of acquisition-related variables may be used as determined by the type of acquisition being undertaken. The acquisition-related variables preferably comprise a component of an acquisition request sent by the entity to the anonymity service. The acquisition request may comprise a purchase request in those instances in which the digital product is offered for sale by the provider. Alternatively, the acquisition request may comprise a request for a free digital product such as shareware or a trial software package as are known in the art. Regardless, at block 302, the anonymity service additionally assigns a unique transaction identification to the acquisition request and associated acquisition-related variables. The anonymity service uses the transaction identification to track and fulfill the acquisition request.

At block 304, the anonymity service uses a cryptographic secret splitting technique to split each of the secrets, i.e., the acquisition-related variables, into a plurality of secret shares. Such secret splitting techniques are well known in the art. In essence, a secret splitting technique takes a secret and divides it up into pieces such that each piece by itself does not allow a holder of that piece to reconstruct the secret. However, a holder in possession of all of the pieces is able to reconstruct the secret.

As an example of secret sharing, assume that a party A wishes to split a secret S into three shares that will be subsequently given to parties B, C and D. In accordance with a preferred embodiment of the present invention, further assume that the secret S is represented as a string of bits having length M. First, A generates two random bit strings, X and Y, each of length M. (Techniques for generating random bit strings are well known in the art of cryptography and are therefore not described in

detail herein.) The secret S is thereafter exclusive-OR'd with X and Y to provide a new bit string Z, also of length M:

$$Z = S \oplus X \oplus Y$$

Thereafter, A provides Z, X and Y (the secret shares) to, for example, B, C and D (the shareholders), respectively. Note that none of B, C or D is able to reconstruct the secret S based solely on their respective share (Z, X or Y). To the contrary, the only way to reconstruct the secret is to combine the secret shares once again:

$$S = Z \oplus X \oplus Y$$

While this is a simple example, it illustrates the basic concept and implementation of secret splitting. For example, a larger number of shareholders may be employed by simply generating additional random bit strings to combine with the secret. One publication teaching a variety of cryptographic secret splitting techniques is "Applied Cryptography" by Bruce Schneier (John Marley & Sons, 1996), the teachings of which are incorporated herein by this reference. Referring back to FIG. 3, the number of secret shares provided at block 304 for each secret is a matter of design choice. Furthermore, the number of secret shares for one secret does not necessarily have to be equal to the number of secret shares for another secret.

At block 306, the secret shares created at block 304 are sent to shareholders for long term storage. While the secret shares could be sent to the shareholders in encrypted form in order to enhance security, the secret shares are sent unencrypted in a presently preferred embodiment. The length of time required by each shareholder to store a corresponding secret share is a matter of design choice and may be dictated, for example, by legal requirements setting the length of time documentation regarding a transaction is to be stored. Once these secrets have been split and sent to the respective shareholders, the anonymity service discards any copies of the secrets. In essence, the anonymity service consumes each secret and distributes the resulting secret shares to corresponding shareholders. So that each secret share can be later recalled by the anonymity service as needed, the anonymity service additionally provides the transaction identification assigned at block 302 to each respective shareholder. Optionally, the anonymity service may provide an identification of the anonymity service itself to each shareholder. Substantially simultaneous to the

transmission of the secret shares to the shareholders, the anonymity service, at block 308, associatively stores the transaction identification and identifications of the shareholders for each secret. That is, the transaction identification is associated with the identifications of the shareholders in possession of secret shares corresponding to that transaction. The transaction identification and shareholder identifications stored by the anonymity service comprise the only information used by the anonymity service to reconstruct secrets corresponding to a given transaction. In this manner, the chances that an adverse party, such as a hacker, discovering an entity's identification, the identification of any providers with whom the entity is dealing with or the identification of any digital products acquired by that entity are substantially minimized.

At block 310, the anonymity service anonymously fulfills the acquisition of the digital product requested by the entity. In this regard, the anonymity service does not disclose the identification of the acquiring entity and the digital product being acquired to any one party. For example, where the entity is acquiring a free software download the anonymity service first reconstructs the identifications of the digital product and a provider of that product by recalling the corresponding secret shares from the appropriate sets of shareholders based on the corresponding transaction identification. The anonymity service thereafter requests the product from the provider without providing the identification of the requesting entity. Upon delivery of the digital product to the anonymity service, the anonymity service thereafter reconstructs the identification of the entity corresponding to that transaction number and provides the digital product to that entity. Where the acquisition by the entity is a purchase of a digital product, the anonymity service again restricts any third party from learning the identification of the entity and the digital product being acquired. This is more fully described with reference to FIGS. 4-7 below.

Once the acquisition of the digital product has been filled by the anonymity service, the only records retained by the anonymity service comprise the transaction identification and the shareholder identifications associated with that transaction identification. If, in the future, a record memorializing the transaction is required (for example, for auditing or legal purposes), an appropriate record can be reconstructed at block 312. To this end, the anonymity service can reconstruct each secret by

requesting the secret shares from the corresponding shareholders. In this manner, the present invention provides accountability to prevent fraud and the like while still providing a greater degree of privacy than previously available.

Referring now to FIGS. 4-7, a technique for purchasing a digital product in accordance with the present invention is illustrated. In particular, an entity wishing to purchase a digital product provides at least three pieces of information to the anonymity service: a provider/product identification, an entity identification, and a price as shown in FIG. 4. Note that, for the sake of simplicity, the provider and product identifications are referred to as single piece of information. Where the instant specification refers to one of either the product or provider identification, the other identification is understood to be available or incorporated. In practice, however, these identifications may be treated separately or in a unified fashion. Regardless, using the secret splitting techniques described above, each of these secrets is split into a corresponding plurality of secret shares as shown in FIG. 4. In particular, the provider/product identification is split into a plurality of secret shares labeled PP1-PPx, the entity identification is split into a plurality of secret shares labeled EI1-EIy, and the price is split into a plurality of secret shares labeled P1-Pz. Note that the values of x, y, and z do not have to be equal to each other and may take on any values as a matter of design choice. Note also that, although not shown in FIG. 4, each secret share illustrated also includes the transaction identification and, optionally, the identification of the anonymity service provider as previously described, either or both of which may be sent in encrypted form. The identification of the anonymity service allows for the use of multiple anonymity services. Each set of secret shares are sent to a corresponding set of shareholders as shown in FIG. 4. In the example shown, the secret shares corresponding to the provider/product identification are sent to a first set of shareholders, the plurality of secret shares corresponding to the entity identification are sent to a second set of shareholders, and the plurality of secret shares corresponding to the price are sent to a third set of shareholders. Once again, note that the anonymity service does not retain copies of any of the secrets but instead retains the transaction identification and the identifications of the shareholders in each set of shareholders corresponding to that transaction identification.

In order to fulfill the purchase of the digital product, the anonymity service must first verify the available credit of the requesting entity. This is further illustrated in FIG. 5. The anonymity service receives credit information from the entity attempting to purchase the digital product. The credit information preferably comprises a credit card number, bank account number or any other type of information used to verify credit, as well as an identification of the financial institution against which the credit may be checked. The credit information may be transmitted to the anonymity service using known encryption techniques. Additionally, based on the transaction identification, the anonymity service requests the plurality of secret shares corresponding to the entity identification from the second set of shareholders. Likewise, the anonymity service requests the plurality of secret shares corresponding to the purchase price from the third set of shareholders. Based on these secret shares, the anonymity service reconstructs the entity identification and the price, which are thereafter transmitted to the credit agency along with the credit information. Based on this information, using known techniques, the credit agency can verify whether an amount of credit equal to the price is available to the entity identified by the entity identification. Note that the credit agency does not receive an identification of the digital product being purchased by the entity. In this manner, the entity is provided with greater privacy with respect to its purchase decisions.

Assuming that a sufficient amount of credit is available to the purchasing entity, the credit agency responds with a credit approval transaction identification which the anonymity service thereafter associates with the transaction identification. Note that the transaction identification can be sent by the anonymity service to the credit agency such that the credit agency, when responding with the credit approval transaction identification, may also inform the anonymity service which transaction the credit approval refers to. Those having ordinary skill in the art will recognize that other techniques for associating the transaction identification with the credit approval transaction identification may be equally employed.

Regardless, once credit approval has been ascertained by the anonymity service, a corresponding amount must be credited to an account of the provider for the purchase of the specific digital product. To this end, the anonymity service and credit agency transmit information to the clearing house as illustrated in FIG. 6. In

particular, the anonymity service reconstructs the seller/product identification by recalling the plurality of secret shares from the first set of shareholders. The seller/product identification is thereafter provided to the clearing house along with the credit approval transaction identification. Substantially simultaneously, the credit agency provides the approved amount (the price) and the credit approval transaction identification to the clearing house as well. Alternatively, the clearing house could request the approved amount from the credit agency based on the credit approval transaction identification received from the anonymity service. Seeing the credit approval transaction identification from both the anonymity service and the credit agency, the clearing house thereafter credits an amount equal to the price to an account of the provider for the sale of the product identified in the provider/product identification. In response, the clearing house associates a clearing house transaction identification with this transaction and sends the clearing house transaction identification back to the anonymity service. In this manner, the provider is subsequently able to ascertain the amount of revenue that it has generated based on the sale of its products without necessarily knowing the identification of the entities that are purchasing these products.

Once the account of the provider has been credited with the proper amount, the anonymity service can complete fulfillment of the purchase by requesting the digital product from the provider. This is further illustrated in FIG. 7. In particular, the anonymity service requests the plurality of secret shares from the first set of shareholders to reconstruct the provider/product identification. Based on the provider/product identification, the anonymity service can send a digital product request to the provider identifying the particular product being requested. In response, the provider sends the requested digital product back to the anonymity service. Additionally, the anonymity service sends the clearing house transaction identification to the provider such that the provider, prior to providing the product to the anonymity service, can verify payment with the clearing house. Once the digital product has been delivered to the anonymity service, the anonymity service thereafter requests the plurality of secret shares from the second set of shareholders in order to reconstruct the entity identification. Based on the entity identification the anonymity service is thereafter able to provide the digital product to the entity. In this manner,

the anonymity service is able to provide the digital product to the entity without providing the identification of the entity to the provider.

In the foregoing specification, the invention has been described with reference to specific embodiments. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the present invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present invention. For example, secure multi-party computing could be used in place of the anonymity service. That is, rather than a single third party managing anonymous transactions, a distributed model may be employed. As known in the art, secure multi-party computation involves passing a digital object (e.g., a piece of data) from one shareholder to the next. Throughout this chain, each shareholder performs an operation such that, by the time the last shareholder has completed its operation, a desired function has been achieved as a cumulative effect of the processing performed by each of the shareholders. For example, secret shares of public keys may be used in this manner to encrypt and decrypt data. As a result, the provider could send the product to the acquiring entity in an encrypted form by letting the shareholders encrypt the product using secure multi-party computation. Thus, in the context of the present invention, the shareholders themselves may implement the product delivery or other functions of the secret shares (if the shareholders are known to each other) using known techniques.

Furthermore, the present invention has been described in terms of single transactions. However, it need not be so limited and could be expanded to handle multiple transactions. For example, where an entity seeks to purchase multiple electronic books from an on-line provider in a single transaction, the anonymity service could split the multiple products (the electronic books) into separate transactions as described above. The splitting of a single transaction comprising multiple items into multiple transactions each comprising a single item also offers a solution to those instances in which one of the items is not available. Without splitting such a single transaction/multiple item request into separate transactions, the unavailability of one of the items would result in the acquiring entity having been

approved for more than necessary. In this case, an amount less than or equal to that which was approved may be paid to the product provider, with any overage credited back by the provider to the transaction identification and, in turn, to an account of the acquiring entity. Alternatively, where such a single transaction/multiple item request is split into separate transactions, this process can be performed on each item separately.

In yet another embodiment, the anonymity service, rather than immediately splitting the secrets up, sending them to the shareholders and then recalling them thereafter for reconstruction, could immediately use the first required secret prior to splitting. For example, when an entity makes a purchase, rather than first splitting the entity's identity and subsequently reconstructing it when needed, the anonymity service could immediately send the entity's identity to the credit agency and thereafter split the entity's identity as needed. Similarly, where a non-purchase transaction occurs, the anonymity service could immediately provide the product identification to the provider and thereafter split the product identification. In either case, the anonymity service again does not retain the secrets after they have been split. In this manner, a degree of added efficiency is provided without a significant sacrifice in security.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential features or elements of any or all the claims. As used herein, the terms "comprises," "comprising," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus.